VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA ÚČETNICTVÍ

ELEKTRONICKÝ PODPIS V ÚČETNÍ PRAXI

ELECTRONIC SIGNATURE IN ACCOUNTING PRACTICE

Student: Lenka Cibulková

Vedoucí bakalářské práce: Doc. Ing. Dagmar Bařinová, Ph.D.

OSTRAVA 2010

VŠB-Technická univerzita Ostrava | Ekonomická fakulta
Katedra Účetnictví | Akademický rok 2010/2011

Zadání bakalářské práce

Student: Lenka Cibulková

Studijní program: Ekonomika a management

Studijní obor: Účetnictví a daně

Téma: Elektronický podpis v účetní praxi

Electronic Signature in Accounting Practice

1. Úvod
2. Právní úprava elektronického podpisu v ČR a EU
3. Elektronický podpis, certifikát a certifikační autorita
4. Uplatnění elektronického podpisu v praxi
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Přílohy

Seznam doporučené odborné literatury:

BUDIŠ, P. [i]Elektronický podpis a jeho aplikace v praxi.[/i] 1. vyd. Olomouc: ANAG, 2008. 160 s. ISBN 978-80-7263-465-1.
VIDINSKÝ, V.; ŠVARCOVÁ, I.; BUDIŠ, P.; LOEBL, Z.; PROCHÁZKOVÁ, B. [i]eGovernment bezpečně.[/i] 1. vyd. Praha: Grada publishing, 2008. 160 s. ISBN 978-80-247-2462-1.
VONDRUŠKA, P.; BOSÁKOVÁ, D.; KUČEROVÁ, A.; PECA, J. [i]Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.[/i] 1. vyd. Olomouc: ANAG, 2002. 144 s. ISBN 80-7263-125-X.

Vedoucí bakalářské práce: Doc. Ing. Dagmar Bařinová, Ph.D.

Datum zadání: 26. listopadu 2010

Datum odevzdání: 29. dubna 2011

Ing. Jana Hakalová, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Místopřísežně prohlašuji, že jsem celou práci, včetně všech příloh, vypracovala samostatně.

Ve …… dne ……_____
Jméno

Chtěla bych poděkovat vedoucí bakalářské práce doc.Ing. Dagmar Bařinové, PhDr. Za poskytnutí odborných připomínek a námětů při řešení dané bakalářské práce. Dále bych chtěla poděkovat Ing. Ondřeji Provalilovi za odborné konzultace.

OBSAH

1 ÚVOD

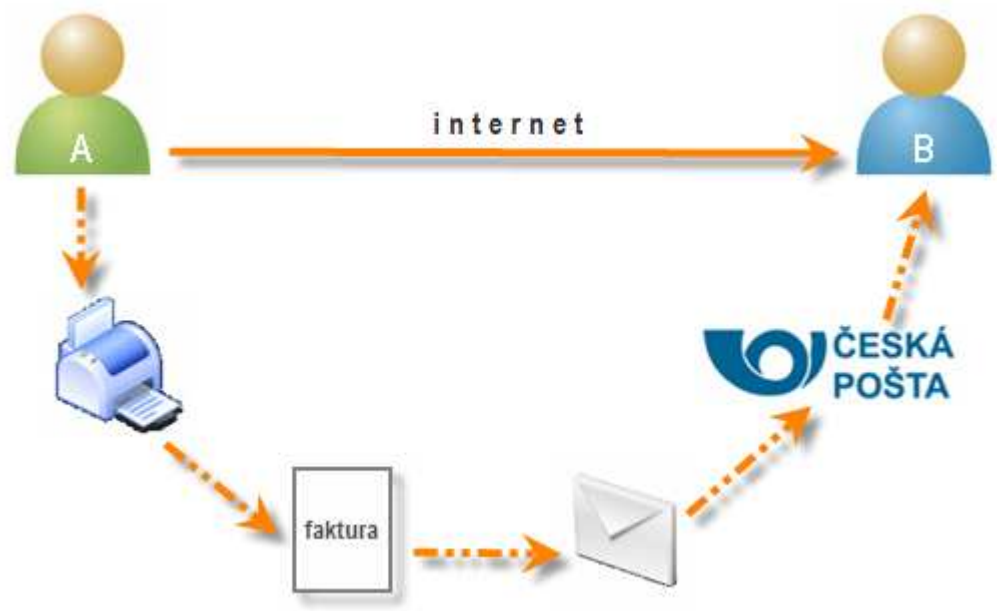
Bakalářská práce se zabývá problematikou elektronického podpisu, která je v dnešní době díky velkému rozvoji internetové komunikace v obchodní i soukromé sféře velmi diskutované a aktuální téma a to hlavně z hlediska bezpečnostního a legislativního. Práce je zaměřena na elektronickým podpis, který splňuje legislativní rámec a to je kvalifikovaný elektronický podpis. Dále se zabývá právní úpravou elektronického podpisu v České republice a Evropské unii, srovnáním akreditovaných poskytovatelů certifikačních služeb v ČR, postupem vydání elektronického podpisu a jeho využitím v praxi, především v e-dokumentech, kde v dané problematice slouží k identifikaci uživatele – zákazníka během komunikace se státní správou a občany, využití elektronického podpisu z účetního hlediska e-fakturace, rozbor elektronických podání (EPO), jež plní funkci daňového přiznání v elektronické podobě, uplatnění v Datových schránkách.

Od doby, kdy jsme se začali seznamovat s dokumenty v elektronické podobě uplynula již řada let a byly shrnuty do pojmu „bezpapírová kancelář“. Zlomovým okamžikem pro elektronický podpis se stal rok 2000, kdy byl přijat zákon č. 227/2000 Sb. o elektronickém podpisu. Do té doby se veškeré důležité dokumenty mohly podepisovat pouze klasickým způsobem. Od data působnosti výše zmíněného zákona je elektronický podpis svou vahou a průkazností postaven na roveň klasickému podpisu a lze jím podepisovat veškeré dokumenty v elektronické podobě.

Až do druhé poloviny roku 2001 nebylo možné elektronický podpis používat ve styku s úřady. To se stalo až po stanovení závazných pravidel prováděcím předpisem. V roce 2002 vstoupila na trh I. Certifikační autorita a s ní i reálná možnost podepisování dokumentu v elektronické podobě pomocí elektronického podpisu. V roce 2005 I. Certifikační autoritu následovali další dva akreditovaní poskytovatelé certifikační služeb – eIdentity, s.r.o. a Postsignum České pošty, s.p..

Přesto, že zde existuje podpora ze strany zákona a příslušné technologie jsou dostupné, je velké množství dokumentů, zejména faktur a dokladů stále vyhotovováno a zasíláno v papírové podobě. Přitom elektronická forma dokumentů má řadu výhod, mezi které patří zejména zpracování, jednoduchá manipulace, výpočetní operace. Účetní doklady jsou dnes ve většině případů zpracovávány na počítači, ale i přesto existuje značná část uživatelů, kteří stále upřednostňují odesílání dokumentů svým partnerům v papírové podobě, archivaci účetních dokladů v papírové formě apod.

Obr. č. 1 Přenos dokladu mezi dvěma subjekty



Zdroj**:** http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html

Obr. č.2 Tok dokladů mezi dvěma subjekty

Zdroj : http://www.isvs.cz/e-podpis-podatelny/papirovy-versus-elektronicky-dokument-27-dil.html

2 PRÁVNÍ ÚPRAVA EL. PODPISU V ČR A EU

Abychom mohli elektronickou komunikaci považovat za rovnocenný ekvivalent běžné papírové komunikaci bylo nutnou podmínkou zavedení takových postupů, přístupů a principů, které by umožnili komerční využití elektronické komunikace. Tyto principy a postupy bylo nutné zakomponovat do obecně platných a závazných dokumentů, zákonů.

Vůbec prvním legislativním dokumentem ve světě, který se zabývá elektronickým podepisováním je UTAH Digital Signature Act. Stát Utah ho přijal 25. února 1995.

2.1 Elektronický podpis v EU

V Evropě směřoval vývoj ke standardizaci prostředí, které by akceptovalo elektronickou komunikaci jako alternativu k dosud obecně používané metodě založené na předávání papírových dokumentů. V říjnu 1997 byla Evropskému parlamentu předložena studie „*O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování*“. Výstupním dokumentem, který Evropský parlament a Rada Evropské unie schválila dne 13. prosince 1999 je *Směrnice 1999/93/ES* (dále jen Směrnice) s cílem usnadnit používání elektronických podpisů a přispět k jejich právnímu uznání v zemích EU. Směrnice je závazná pro všechny členské země EU, které požadavky dané směrnicí více či méně úspěšně transformují do svých lokálních legislativ.

V současné době se problematikou elektronického podpisu v rámci EU zabývá sdružení FESA (*Forum of European Supervisory Authorities for Electronic Signatures*). FESA je evropské fórum institucí, které na národní úrovni vykonávají akreditační a dozorovou činnost podle Směrnice 1999/93/ES o zásadách společenství pro elektronické podpisy. Členem je v současné době více než 20 států. Cílem fóra je podpora vzájemné spolupráce a koordinace svěřených kompetencí na mezinárodní úrovni, vytváření jednotných stanovisek a komunikace s orgány EU, především Evropskou komisí. Zástupci členských institucí FESA se schází pravidelně třikrát do roka ke schválení společných stanovisek a k projednání úkolů vzešlých z dosavadní praxe jednotlivých institucí.[1]

Směrnice je zpracována velmi podrobně a kromě otázky definice, tvorby a ověření elektronického podpisu se zabývá právní uznatelností elektronického podpisu v zemích EU,

[1] http://aplikace.mvcr.cz/archiv2008/micr/eu/fesa.htm

procesy vydávání certifikátů, způsoby akreditace včetně dalších služeb, které poskytovatelé certifikačních služeb nabízí. Nyní se zaměřím na nejzajímavější body směrnice.

Směrnice byla vypracována tak, aby byly dodrženy tři následující principy :

- Technologická neutralita, to znamená, že směrnice výslovně nehovoří o žádné konkrétní technologii, což otevírá prostor pro řadu dalších nejenom biometrických metod,
- Pro poskytovatele certifikačních služeb není primárně definováno žádné schéma pro autorizaci k provádění těchto služeb, tak aby v budoucnu existovala principiální možnost technologických inovací,
- Určení zákonné platnosti zaručených elektronických podpisů tak, aby nemohla být popřena jejich platnost pouze na základě toho, že jsou v elektronické podobě.[2]

Jedním z hlavních přínosů směrnice je sjednocení terminologie na elektronický podpis.

V rámci Směrnice se rozumí :

1) **elektronickým podpisem** údaj v elektronické podobě, kterým je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti,
2) **zaručeným elektronickým podpisem** elektronický podpis, který splňuje tyto požadavky :
   a) je jednoznačně spojen s podepisující osobou,
   b) umožňuje zjistit totožnost podepisující osoby,
   c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou, a
   d) je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoli následnou změnu těchto dat,
3) **podepisující osobou** jakákoli osoba, která má prostředek pro vytváření podpisu a která jedná na svůj účet nebo na účet fyzické či právnické osoby nebo subjektu, které zastupuje,
4) **daty pro vytváření podpisu** jedinečná data, jako jsou kódy nebo soukromé šifrovací klíče, které podepisující osoba používá k vytvoření elektronického podpisu,

[2] Budiš, P. *Elektronický podpis a jeho aplikace v praxi*. 2008. S. 103.

5) **prostředkem pro vytváření podpisu** konfigurovaný softwarový nebo hardwarový prostředek pro využití dat pro vytváření podpisu,

6) **prostředkem pro bezpečné vytváření podpisu** prostředek pro vytváření podpisu, který splňuje požadavky uvedené v samostatné části Směrnice,

7) **daty pro ověřování podpisu** data, jako kódy nebo veřejné šifrovací klíče, které se používají pro ověřování elektronického podpisu,

8) **prostředek pro ověřování podpisu** konfigurovaný softwarový nebo hardwarový prostředek pro využití dat pro ověření podpisu,

9) **osvědčením** (certifikátem) elektronické potvrzení, které spojuje data pro ověřování podpisu s určitou osobou a potvrzuje totožnost této osoby,

10) **kvalifikovaným osvědčením** osvědčení, které splňuje požadavky uvedené v příloze Směrnice, které vydává ověřovatel, jenž splňuje požadavky uvedené v samostatné části Směrnice,

11) **ověřovatelem** subjekt nebo právnická či fyzická osoba, která vydává osvědčení nebo poskytuje jiné služby související s elektronickými podpisy,

12) **produktem pro elektronický podpis** hardware nebo software nebo jeho odpovídající části, které jsou určeny k tomu, aby je ověřovatel používal pro poskytování služeb souvisejících s elektronickými podpisy, nebo které jsou určeny pro vytváření nebo ověřování elektronických podpisů.

2.2 Elektronický podpis v ČR

V České republice nabyl dne 1. října 2000 platnost zákon č. 227/2000 Sb., o elektronickém podpisu (dále jen ZoEP) a byl vytvořen na základě směrnice Evropské unie 1999/93/EC. V rámci EU se tak Česká republika stala již třetí zemí, kde vstoupil v platnost zákon o užívání elektronického podpisu. Tento zákon se zabývá právní úpravou elektronického podpisu, regulací poskytovaných služeb souvisejících s elektronickým podpisem, stanovení povinností, jejich kontrola a ukládání sankcí nebudou-li povinnosti dodrženy. Definuje rozdíl mezi obecným certifikátem a certifikátem kvalifikovaným.

Dohled nad dodržováním zákona o elektronickém podpisu zastává v současné době Ministerstvo vnitra ČR. Mezi jeho hlavní povinnosti patří :

- dozor nad dodržováním zákona o elektronickém podpisu,
- udělování akreditací poskytovatelům certifikačních služeb a
- vyhodnocování shody nástrojů elektronického podpisu s požadavky stanovenými zákonem.

Od roku 2000 byl ZoEP již několikrát novelizován:[3]

- **zákon č. 226/2002 Sb.,** ze dne 9.května 2002 – Změna § 11 ZoEP upravující podmínky používání elektronického podpisu a certifikátů v oblasti orgánů veřejné moci,
- **zákon č. 517/2002 Sb.,** ze dne 14. listopadu 2002 – Upravuje ZoEP na základě provedení některých opatření v soustavě ústředních orgánů státní správy, nahrazení slova „Úřad pro ochranu osobních údajů“ a „Úřad“ slovem „Ministerstvo informatiky“,
- novela **zákona o elektronickém podpisu č. 440/2004 Sb**., nabyla platnost 26. července 2004**.** Tímto předpisem se nově zavádí pojem „kvalifikované časové razítko“, prokazující existenci elektronického dokumentu v čase a pojem „elektronické značka“, kterou mohou označovat svá data i právnické osoby nebo organizační složky státu za použití automatizovaných postupů. Pro elektronickou značku se stejně jako pro elektronický podpis používá technologie digitálních podpisů,

Naposledy byl ZoEP novelizován **zákonem č. 223/2009 Sb**., zákonem č. **227/2009 Sb.** a zákonem č. **281/2009 Sb.**

Další nařízení a vyhlášky :

- **Nařízení vlády č. 304/2001 Sb.** Ze dne 25. července 2001 – upravuje ZoEP, zejména elektronických podatelen v rámci orgánů veřejné moci tak, aby bylo zajištěno přijímání podání v elektronické podobě při využití kvalifikovaných certifikátů dle výše uvedeného zákona.

[3] http://www.mvcr.cz/e-podpis-legislativa.aspx

- **Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb**. ze dne 3. října 2001. Vyhláška upřesňuje podmínky § 6 ZoEP , který specifikuje povinnosti poskytovatele certifikačních služeb vydávajících kvalifikované certifikáty a § 17 ZoEP, definující prostředky pro vytváření a ověřování zaručených elektronických podpisů.

- **Nařízení vlády č. 495/2004 Sb.,** kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Tímto nařízením ze dne 25. srpna 2004 vláda schválila nařízení o elektronických podatelnách. Orgány státní moci jsou povinny zřídit E-podatelny (v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu), vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací. Nařízení vlády nabylo účinnosti k 1. lednu 2005.

- **Vyhláška č. 496/2004 Sb.,** k elektronickým podatelnám navazuje na nařízení vlády č. 495/2004 Sb.a nařizuje orgánům státní moci elektronickou podatelnu zřídit. Dále upravuje postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny.

- **Vyhláška č. 378/2006 Sb**., o postupech kvalifikovaných poskytovatelů certifikačních služeb ze dne 2. srpna 2006. První část vyhlášky je určena poskytovatelům certifikačních služeb a obsahuje požadavky na jejich postupy při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Druhá část se vztahuje na označující osoby, zejména na orgány veřejné moci – obsahuje požadavky na ochranu soukromých klíčů, které se používají při vytváření elektronických značek.

První část vyhlášky nabývá účinnosti 17.8.2006, druhá část nabývá účinnosti 1.11.2006.

2.2.1 Zákon č. 227/2000 Sb., o elektronickém podpisu

V § 1 ZoEP je vymezen účel zákona, to znamená používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za jejich porušení.

V § 2 jsou vymezeny některé základní pojmy :

- daty pro vytváření elektronických podpisů se rozumí - jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,
- daty pro ověřování elektronických podpisů - jedinečná data, která se používají pro ověření elektronického podpisu,
- prostředkem pro vytváření elektronických podpisů – technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů

Elektronický podpis (EP) jako : „*Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo s ní jsou logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.*“

Zaručený elektronický podpis (ZEP) je vyšší formou elektronického podpisu a musí splňovat následující požadavky :

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Kvalifikovaný podpis vzniká použitím zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu.

Uznávaný podpis vzniká použitím zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, který vydal akreditovaný poskytovatel certifikačních služeb.

V § 3 je vymezen soulad s požadavky na podpis

- datová zpráva je podepsána je-li opatřena elektronickým podpisem,
- použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

§ 4 soulad s originálem

- použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit.

V § 5 jsou uvedeny povinnosti podepisující osoby.

Podepisující osoba je povinna :

a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití, to znamená

b) uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu,

c) podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

To znamená, první povinnost podepisující osoby je zaměřena především na bezpečné zacházení se soukromým klíčem, případně s prostředky pro podepisování. Druhá ukládá podepisující osobě povinnost ihned sdělit poskytovateli certifikačních služeb, že došlo ke kompromitaci soukromého klíče. Za škodu způsobenou podle bodu c) odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn. (Zákon č. 40/1964 Sb., občanský zákoník)

§ 6 jsou vymezeny povinnosti poskytovatele certifikačních služeb (PCS) vydávajícího kvalifikované certifikáty používat bezpečné systémy a nástroje elektronického podpisu a

zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují. Nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou. Tto musí být ověřeno Úřadem pro ochranu osobních údajů.

V § 11 je stanoveno, že v oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, stanoví ministerstvo prováděcím právním předpisem.

Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

Orgán veřejné moci přijímá a odesílá datové zprávy prostřednictvím elektronické podatelny.

V § 12 jsou uvedeny náležitosti kvalifikovaného certifikátu

1) Kvalifikovaný certifikát musí obsahovat :
    - označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,
    - obchodní jméno poskytovatele certifikačních služeb, jeho sídlo a údaj, že byl vydán v České republice,
    - jméno a příjmení podepisující osoby, případně pseudonym s příslušným označením,že se jedná o pseudonym podepisující osoby,
    - zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
    - data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
    - zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,
    - číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

- počátek a konec platnosti kvalifikovaného certifikátu,
- případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,
- případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

2) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

2.2.2 Uznávání kvalifikovaných certifikátů pro elektronický podpis v rámci EU

Dne 16.102009 bylo přijato rozhodnutí Komise 2009/67/ES, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice EP a Rady 2006/123/ES o službách na vnitřním trhu, které nabylo účinnosti dne 28.12.2009.

Tímto dnem nastala povinnost uznávat kvalifikované certifikáty vydané poskytovateli certifikačních služeb usazenými v jiných státech EU i pro orgány veřejné moci. Předpokladem je, že stát ve kterém byl certifikát vydán zveřejní Trusted Services Lists (TSL). TSL slouží k ověřování, zda certifikát vydaný v členském státu EU jako kvalifikovaný je kvalifikovaným certifikátem ve smyslu Směrnice 1999/93/ES.

Seznam adres všech publikovaných TSL členských států by měl být zveřejněn v „seznamu TSL“ (LOTL – List of the Listsú. Seznam TSL je dostupný na internetové adrese (https://ec.europa.eu).

Česká republika se stala prvním státem Evropské unie, kterému byl Evropskou komisí TSL notifikován. Ministerstvo vnitra připravilo webovou aplikaci, která usnadní ověřování certifikátů z jiných členských států. Po nahrání souboru s certifikátem vyhodnotí aplikace na základě informací publikovaných v TSL jednotlivých členských států, zda byl tento certifikát vydán jako kvalifikovaný. Aplikace je volně dostupná na adrese http://tsl.gov.cz/certig/. Vzhledem k tomu ne všechny členské státy stihly svá TSL publikovat v požadovaném termínu a k naplnění seznamu TSL (LOTL) bude docházet průběžně doporučuje Ministerstvo vnitra při každém použití aplikace zkontrolovat, se kterými TSL aplikace v daném okamžiku

pracuje. V případě nenalezení TSL konkrétního stát je možné se obrátit s žádostí o pomoc při ověření certifikátu na emailovou adresu Ministerstva vnitra (okkisvs@mvcr.cz).

Pro držitele českých kvalifikovaných certifikátů to znamená, že důvěryhodnost jejich certifikátů mohou nyní ověřit i zahraniční osoby a dle Směrnice k němu tedy budou přistupovat obdobně, jako ke kvalifikovaným certifikátům vydaným ve své zemi.

3 ELEKTRONICKÝ PODPIS, CERTIFIKÁT A CERTIFIKAČNÍ AUTORITA

Pro lepší orientaci v problematice elektronického podpisu si nejdříve připomeneme pojmy, které s elektronickým podpisem souvisí. Při jejich definování vycházíme ze zákona č. 227/2000 Sb., o elektronickém podpisu.

3.1 Definice a pojmy

Elektronický podpis (EP)

Zákon definuje elektronický podpis jako : „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo s ní jsou logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.*“

Zaručený elektronický podpis (ZEP)

Je vyšší formou elektronického podpisu a musí splňovat následující požadavky :

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Certifikát

Jedná se o datovou zprávu, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu.

Certifikát může do jisté míry chápat jako obdobu průkazu totožnosti, například občanského průkazu.

Kvalifikovaný certifikát

Splňuje všechny požadavky na elektronický podpis dané Zákonem o elektronickém podpisu (§ 12 ZoEP-ČR) . Lze jej využít výhradně pro podepisování dat a je podmínkou bezpečné komunikace občanů se státní správou. Elektronický podpis založený na Kvalifikovaném certifikátu je automaticky akceptován všemi úřady státní správy. Je určen k ověřování elektronického podpisu, přesněji pro identifikaci a autentizaci podepisující osoby a tím pro zajištění integrity zprávy (aby se spolehlivě poznalo, zda byla či nebyla zpráva pozměněna).

Komerční certifikát

Není spojen se zákonem o elektronickém podpisu a není uznáván státní správou pro podepisování.

Kvalifikované časové razítko

Je datová zpráva vydaná akreditovaným poskytovatelem certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Certifikační autorita (CA)

Certifikační autorita, nebo-li poskytovatel certifikačních služeb je důvěryhodná instituce, která ověřuje identitu osob a vystavuje a zneplatňuje certifikáty. Tomuto subjektu musí důvěřovat obě strany, které si mezi sebou chtějí vyměňovat podepsané nebo šifrované zprávy.

CRL (Seznam zneplatněných certifikátů)

Jedná se o listinu, na které jsou uvedeny zneplatněné certifikáty, jejichž běžná doba platnosti ještě nevypršela. CRL je veřejně přístupný dokument, který je stejně jako certifikát chráněný podpisem Certifikační autority. Certifikační autorita tento seznam vydává v pravidelných intervalech a certifikát je na nich uveden do doby, než jeho platnost řádně vyprší.

Validace

Ověření integrity neboli narušenosti zprávy nebo její zvolené části.

Akreditace

Akreditace znamená oficiální uznání, že subjekt akreditace (poskytovatel certifikačních služeb) je schopen provádět specifické činnosti.

USB token

Zařízení připomínající USB paměť, které sloužící k bezpečnému uložení soukromého klíče a certifikátu.

Symetrická kryptografie

Využívá pouze jediný šifrovací klíč. To znamená, že stejný klíč je použit k zašifrování zprávy na straně odesílatele a stejný klíč bude použit i při rozšifrování zprávy na straně příjemce.

Asymetrická kryptografie

V asymetrické kryptografii se užívá dvojice klíčů a to soukromý a veřejný klíč. Jiný klíč se použije pro zašifrování a jiný klíč pro dešifrování dat.

3.2 Bezpečná komunikace

Elektronický podpis je jedním z nástrojů pro zajištění bezpečné elektronické komunikace. Aby elektronická komunikace ve sféře státní správy, financí, zdravotnictví, obchodu a dalších odvětvích byla bezpečná je třeba přenášená data maximálně chránit a zaručit tak důvěrnost, integritu a nepopíratelnost zasílaných dat.

- Důvěrnost informací – zajistit přístup k informacím pouze autorizovaným subjektům, tedy těm, kterým je zpráva určena.
- Integrita – systém musí zabezpečit informace proti modifikaci, změně přenášených dat,
- Nepopíratelnost – schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu z autorství, vlastnictví, odesílání, případně přijetí zprávy.

Zabezpečení informací v elektronické komunikaci uskutečňuje za pomocí kryptografie, tedy šifrování.

Rozlišujeme dvě šifrovací metody :

- Symetrickou kryptografii
- Asymetrickou kryptografiii

3.2.1 Symetrická kryptografie

Metoda symetrické kryptografie využívá jediného klíče k zašifrování zprávy na straně odesílatele a toho samého klíče na straně příjemce. To znamená, že obě strany, které spolu komunikují, vlastní stejný klíč a před začátkem komunikace je tedy nutné si mezi sebou příslušný klíč předat. Nevýhodou je tedy obtížná distribuce a předávání mezi uživateli, kteří spolu chtějí tímto způsobem komunikovat.

3.2.2 Asymetrická kryptografie

Asymetrická kryptografie užívá dvojice klíčů. Tuto dvojici klíčů si uživatel vygeneruje pomocí dostupných softwarových produktů a stává se jejich jediným majitelem. Označují se jako párová data (soukromý a veřejný klíč). V zájmu majitele je maximální ochrana soukromého klíče (čipová karta, USBtoken atd) naproti tomu veřejný klíč můžeme sdělit prakticky komukoliv. Lze-li jeden z klíčů zveřejnit aniž by bylo možné druhý z dvojice klíčů odvodit – mluvíme o kryptografii s veřejným klíčem.

3.3 Elektronický podpis

Jak již bylo několikrát zmíněno, zákon 227/2000 Sb., definuje elektronický podpis jako : „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo s ní jsou logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.*“

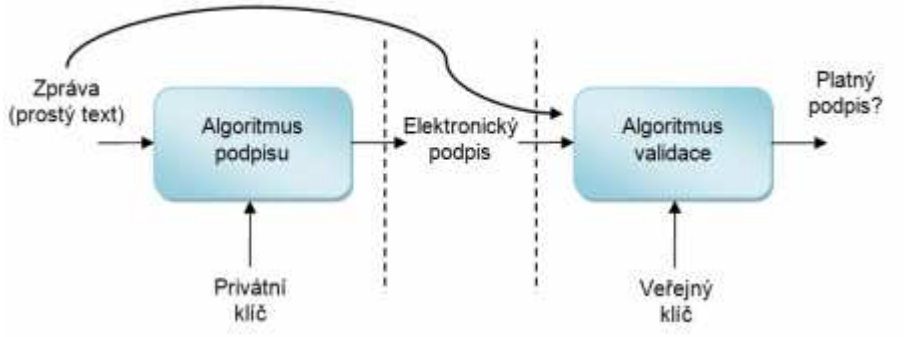
3.3.1 Elektronické podepisování

Elektronické podepisování se provádí pomocí hash funkce, kdy se vytvoří takzvaný otisk zprávy, který je zašifrován pomocí soukromého klíče a připojen k podepisované zprávě. Příjemce zprávy tento otisk dešifruje s pomocí veřejného klíče, který je obsažen v certifikátu a opět za pomocí hash funkce vygeneruje ze zprávy nebo datového souboru nový otisk, přičemž oba porovná a v případě, že jsou totožné, je zřejmé, že nedošlo k žádným pozdějším úpravám zasílaných informací a odesílatel zprávy byl identifikován a ověřen.

Hash funkce - jedná se o jednosměrnou transformaci, která variabilním vstupních hodnotám přiřadí jednoznačnou výstupní hodnotu (řetězec) pevné délky.
Délka hodnoty hash je dána typem použitého hash algoritmu a nemění se v závislosti na délce vlastní zprávy. V praxi se využívají např. hashovaní funkce MD-5, SHA-1, SHA-2.
Bezpečnost hashovacích funkci patří ke klíčových bezpečnostním parametrům elektronického podpisu a vzhledem k tomu, že dochází k prudkému vývoji v oblasti kryptoanalýzy hashovacích funkcí vydal NBÚ[4], který provádí dohled v oblasti kryptografické ochrany prohlášení, ve kterém již nedoporučuje nadále používat hashovaní funkce s výstupem menším než 160 bitů (např. MD-4, MD-5) a doporučuje přechod z hashovaní funkce SHA-1 na SHA-2.

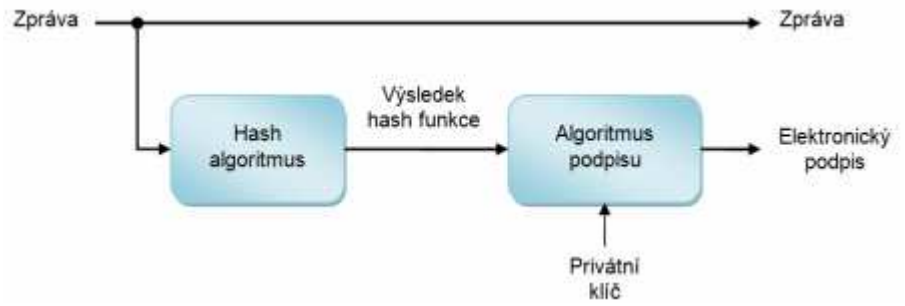
[4] http://www.nbu.cz

Obr. č.3 Proces vytváření a ověřování elektronického podpisu



Zdroj : http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/

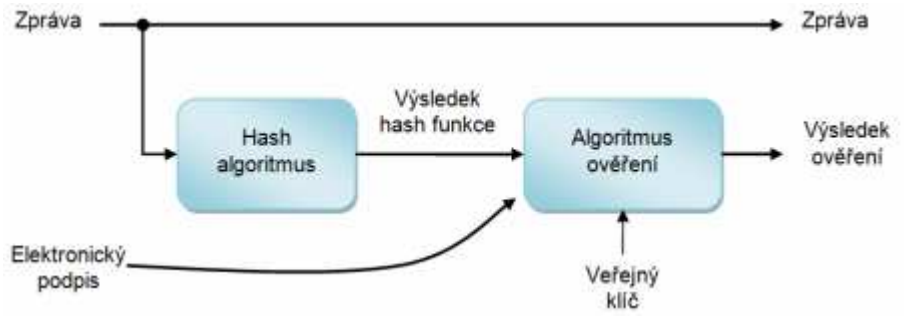
Obr. č.4 Proces vytváření elektronického podpisu



Zdroj : http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/

Odesílatel zprávy nejdříve vypočte hash hodnotu zprávy a potom ji teprve zašifruje svým privátním klíčem a tím vznikne elektronický podpis zprávy.

Obr. č.5 Proces ověření elektronického podpisu



Zdroj : http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/

Příjemce zprávy ověří podpis výpočtem hash hodnoty zprávy a porovná s dešifrovanou hodnotou z elektronického podpisu. V případě shody, je zřejmé, že zpráva byla podepsána odesílatelem a nebyla po jejím podepsání nijak pozměněna, jedná se o tzv. integritu zprávy.

Výhody elektronického dokumentu

- úspora nákladů na vyhotovení dokladu,
- úspora nákladů za poštovné,
- úspora lidské práce,
- zrychlení komunikace,
- automatizace účetnictví,
- zpřehlednění procesů,
- zamezení vzniku chyb,
- zkrácení doby splatnosti faktur,
- usnadnění a urychlení kontroly,
- šetrnost k životnímu prostředí,
- napojení na elektronický platební styk

Nevýhody elektronického dokumentu

- ochrana dokumentu,
- zabezpečení dokumentu,
- finanční náročnost zavedení

3.4 Certifikát

Certifikát je datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit jejich identitu.

3.4.1 Typy certifikátů

Rozlišujeme dva typy certifikátů :

- Komerční certifikáty
- Kvalifikované certifikáty

Komerční certifikáty

Komerční certifikát není vymezen zákonem o elektronickém podpisu a nelze jej tedy využít pro komunikaci se státní správou. Zato jej můžeme využít pro šifrování, přihlašování do aplikací, prokazování identity a autentizace, zabezpečení apod. Například pro přihlášení do datové schránky nebo elektronického bankovnictví použije uživatel svůj komerční osobní certifikát. Mezi komerční certifikáty patří i takzvané serverové certifikáty, které se využívají pro autentizaci webových serverů (protokol http).

Kvalifikované certifikáty

Jedná se o certifikáty, které byly vydané v souladu se zákonem o elektronickém podpisu a jsou určeny výhradně pro ověření elektronického podpisu a nelze je použít při šifrování zpráv. Použití kvalifikovaného certifikátu je podmínkou bezpečné komunikace občanů s státní správou.
Mezi kvalifikované certifikáty patří i takzvané kvalifikované systémové certifikáty. Zde ovšem nemluvíme o elektronickém podpisu, ale hovoříme o elektronické značce. Užití elektronické značky je spojeno především s elektronickými podatelnami a slouží pro automatizované podepisování.

Kvalifikovaný systémový certifikát (elektronická značka)

Z technologického hlediska není mezi elektronickou značkou a zaručeným elektronickým podpisem rozdíl. Odlišnost je pouze z právního hlediska. Zatímco elektronický podpis vytváří fyzická osoba, elektronickou značkou může datové zprávy označovat i právnická osoba nebo organizační složka státu a můžeme ji přirovnat k otisku úředního razítka. Elektronickými značkami jsou dokumenty opatřovány automatizovaně.

Kvalifikované časové razítko

Kvalifikované časové razítko spojuje data v elektronické podobě s určitým časovým okamžikem. Důvěryhodným a ověřitelným způsobem tak zajišťuje prokazatelnost, kdy dokument vznikl, kdy byl přijat či odeslán a kdy byl podepsán. Zároveň umožňuje u elektronických transakcí, formulářů, elektronických podpisů, archivovaných dat prokázat jejich existenci v určitém čase a například elektronický podpis, byl ve chvíli připojení k podpisu platný. A to i dlouhé roky po té, co jeho platnost vypršela.

Obr. č.6 důvěryhodný dokument

Zdroj : http://www.secustamp.com/cs/casove-razitko

3.5 Certifikační autorita (CA)

Certifikační autorita je subjekt, který vydává certifikáty veřejných klíčů ostatním subjektům i osobám. Vydávání certifikátů se řídí certifikační politikou, dokumentem, ve kterém jsou stanoveny podmínky pro vydání certifikátu, způsob používání certifikátu a údaje obsažené v certifikátu. CA svou autoritou potvrzuje pravdivost údajů uvedených ve veřejné části klíče, který je volně dostupný.

3.5.1 Kvalifikovaná certifikační autorita

Kvalifikovaná certifikační autorita je definována zákonem o elektronickém podpisu a seznam akreditovaných certifikačních autorit, které mohou vydávat kvalifikované certifikáty zveřejňuje Ministerstvo vnitra České republiky na svých internetových stránkách.

Tab. č.1 Akreditovaní poskytovatelé certifikačních služeb

Poř. číslo	**Poskytovatelé certifikačních služeb**	**Kvalifikované služby – vydávání :**	**Zahájení vydávání**
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	kvalifikovaných certifikátů; kvalifikovaných systémových certifikátů; kvalifikovaných časových razítek.	03/2002 02/2006 02/2006
2.	Česká pošta, s. p., identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	kvalifikovaných certifikátů; kvalifikovaných systémových certifikátů; kvalifikovaných časových razítek.	09/2005 04/2005 07/2009
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	kvalifikovaných certifikátů; kvalifikovaných systémových certifikátů; kvalifikovaných časových razítek.	08/2005 08/2005 08/2010

Zdroj :www.mvcr.cz

Každý z výše uvedených poskytovatelů má na svých internetových stránkách potřebné informace o nabízených certifikačních službách a záleží pouze na nás pro kterého z nich se rozhodneme.

Rozhodovat se můžeme například podle následujících kritérií:

- dostupnost registračního místa pro žadatele o certifikát,
- cena certifikátu - požaduji/nepožaduji čipovou kartu,
- přívětivost aplikací a jejich použitelnost na různých platformách (např. žádosti o vydání certifikátu),
- složitost/jednoduchost postupu při získání certifikátu,
- srozumitelnost informací, které poskytovatel zveřejňuje.

Před podáním žádosti o vydání certifikátu by jsme se měli také seznámit s Certifikační politikou příslušného poskytovatele, případně s certifikačními politikami více poskytovatelů a porovnat nabízené služby jednotlivých poskytovatelů.

Srovnání nabízených služeb akreditovaných poskytovatelů

Tab. č.2 I. Certifikační autorita

Poskytovatel CA	I.CA
Počet registračních autorit	Více než 300 + mobilní registrační autorita
Typy vydávaných certifikátů	Kvalifikovaný certifikát,kvalifikovaný systémový certifikát, komerční certifikát,komerční certifikát pro server
Délka kryptografického klíče	2048 bitů
Doba platnosti certifikátu	12 měsíců (365 dní)
Cena kvalifikovaného certifikátu Standard	495 Kč
Cena komerčního certifikátu Standard	395 Kč
Nabízí kvalifikované časové razítko	ano
Bezpečné úložiště klíče	USB Token, čipová karta
Způsob ověření totožnosti	občanský průkaz + další doklad totožnosti s fotografií, u podnikatele (OSVČ) dále doklad o existenci společnosti
Způsob generování žádosti	on-line na webových stránkách offline pomocí aplikace ICANEWCERT
Způsob vydání certifikátu	osobně, e-mailem
Způsob obnovy certifikátu	elektronicky (pouze v době jeho platnosti)
Způsob zneplatnění certifikátu	on-line, e-mailem, osobně
Aktualizace CRL	maximálně za 24 hodin od vydání předchozího CRL (zpravidla 8 hodin)

Tab. č.3 Česká pošta, s.p.

Poskytovatel CA	Česká pošta, s.p. - PostSignum
Počet registračních autorit	945 + 7 mobilních registračních autorit
Typy vydávaných certifikátů	Kvalifikovaný certifikát, kvalifikovaný systémový certifikát, komerční certifikáty (osobní, serverový, šifrovací)
Délka kryptografického klíče	2048 bitů
Doba platnosti certifikátu	12 měsíců (365 dní)
Cena kvalifikovaného certifikátu	396 Kč
Cena komerčního certifikátu	348 Kč
Nabízí kvalifikované časové razítko	ano
Bezpečné úložiště klíče	USB token
Způsob ověření totožnosti	Jeden doklad totožnosti, dále doklad o existenci společnosti Fyzická osoba nepodnikající dva doklady totožnosti
Způsob generování žádosti	on-line na webových stránkách offline pomocí aplikace Postsignum Tool
Způsob vydání certifikátu	osobně
Způsob obnovy certifikátu	Elektronicky, osobně
Způsob zneplatnění certifikátu	Osobně, telefonicky, faxem,e-mailem,poštou,
Aktualizace CRL	po zneplatnění, jinak min 1x za 12 hodin

Tab.č.4 eIdentity, a.s.

Poskytovatel CA	eIdentity, a.s.
Počet registračních autorit	4 + mobilní registrační autorita
Typy vydávaných certifikátů	kvalifikovaný certifikát, kvalifikovaný systémový certifikát, komerční certifikát, komerční serverový certifikát
Délka kryptografického klíče	2048 bitů
Doba platnosti certifikátu	12 měsíců (365 dní)
Cena kvalifikovaného certifikátu	474 Kč
Cena komerčního certifikátu	354 Kč
Nabízí kvalifikované časové razítko	ano
Bezpečné úložiště klíče	není v nabídce
Způsob ověření totožnosti	Jeden doklad totožnosti, dále doklad o existenci společnosti fyzická osoba nepodnikající dva doklady totožnosti
Způsob generování žádosti	on-line na webových stránkách offline pomocí aplikace Postsignum Tool
Způsob vydání certifikátu	osobně
Způsob obnovy certifikátu	elektronicky, osobně
Způsob zneplatnění certifikátu	osobně, telefonicky, faxem,e-mailem,poštou,
Aktualizace CRL	Min 1x za 24 hod, zpravidla co 4 hodiny

I. Certifikační autorita (I.CA)

I.CA zahájila poskytování certifikačních služeb již v roce 1996 jako součást produktového portfolia společnosti PVT, a.s. Počátkem roku 2001 byla založena dceřiná společnost PVT, a.s. s názvem První certifikační autorita, a.s.. která převzala od mateřské společnosti veškeré činnosti bezprostředně související s poskytováním certifikačních služeb.

V roce 2002 byla společnosti udělena Úřadem pro ochranu osobních údajů akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona 227/2000 Sb., o elektronickém podpisu a I.CA[5] tak zahájila vydávání kvalifikovaných certifikátů určených zejména pro komunikaci v oblasti orgánů veřejné moci.

V roce 2006 udělilo Ministerstvo informatiky ČR společnosti rozšířenou akreditaci ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 01. 02. 2006 v oblasti poskytování služeb kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek.

Pro zajištění optimální dostupnosti svých nabízených služeb provozuje I.CA infrastrukturu registračních autorit a to :

- síť veřejných registračních autorit na pobočkách CzechInvestu, omezeně na pobočkách ČSOB, a.s.,
- registrační autority na pobočkách krajských úřadů a ve velkých městech.

Kromě poskytování jednotlivých typů certifikátu nabízí další produkty a služby jako :

TWINS

Produkt, který umožňuje uživateli využívat elektronický podpis (osobní kvalifikovaný certifikát) a zároveň službu autentizace a šifrování (komerční certifikát). Žádost o oba certifikáty je provedena na jednom formuláři. V systému je zajištěna vazba mezi oběma certifikáty a vydání certifikátu TWINS je uskutečněno najednou. V případě obnovy je proces uskutečněn automatizovaně prostřednictvím informačního e-mailu – bez nutnosti návštěvy klienta na registrační autoritě.

[5] http://ica.cz

Nárůst požadavků na certifikáty TWINS v roce 2009 byl vyvolán zahájením provozu datových schránek a dalšími projekty jako e-Fakturace, e-Archiv apod.

e-Já = e-Me

jedná se o kombinaci produktu TWINS a čipové karty Starcos 3.0 a nabízí klientovi možnost uložení obou certifikátů na bezpečné medium s přístupem pomocí PIN a v případě nutnosti použití hesel pro zneplatnění certifikátů. Na tomto médiu je produkt e-Já libovolně přenositelný a není tedy vázán na konkrétní počítač.

V současné době je I.CA největším poskytovatelem komplexních služeb vydávání a správy certifikátů v ČR a své služby poskytuje také na Slovensku. Společnost je vlastněna několika významnými společnostm jako je Česká spořitelna, a.s., ČSOB, a.s., Telefónica O2 CR, a.s., Asseco, a.s. a Státní tiskárna cenin s.p.

Počty vydaných certifikátů jsou dnes evidovány řádově ve statisících. O tom svědčí stále rostoucí zájem o elektronickou komunikaci s využitím elektronického podpisu.

I.CA, a.s., již vydala 300.000 kvalifikovaných certifikátů a oproti roku 2008 se tak počet vydaných kvalifikovaných certifikátů ztrojnásobil.

V roce 2009 pokračoval také nárůst poskytování služeb časové autority (kvalifikovaných časových razítek). Celkový počet vydaných kvalifikovaných časových razítek v roce 2009, vzrostl oproti roku 2008 z 10,5 na 12,6 milionů tj. nárůst o 20%. (www.ica.cz)

Česká pošta, s.p. - Postsignum

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb dne 3.8.2005 na základě akreditace udělené Ministerstvem informatiky ČR. Certifikační autorita Postsignum[6] poskytuje služby vydávání kvalifikovaných, komerčních certifikátů a poskytování kvalifikovaného časového razítka.
Mezi další služby, které nabízí je zřízení datové schránky včetně doplňkových produktů jako Bezpečný klíč, který umožňuje chráněný přístup k datové schránce. Česká pošta nabízí tři druhy Bezpečného klíče.
Bezpečný klíč k datové schránce KOMPLET

[6] http://postsignum.cz

- je určen zákazníkům, kteří nevlastní kvalifikovaný ani komerční certifikát, chtějí zvýšit bezpečnost přístupu ke svým datovým schránkám a zároveň chtějí svou elektronickou komunikaci opatřit zaručeným elektronickým podpisem. Balíček obsahuje USB token iKey 4000, licenci obslužného software, instalační CD a poukázky na vydání osobního kvalifikovaného a komerčního certifikátu.

Bezpečný klíč k datové schránce PŘÍSTUPOVÝ

- je určen pro zákazníkům, kteří již vlastní kvalifikovaný certifikát a chtějí pouze zvýšit bezpečnost přístupu ke svým datovým schránkám. Balíček obsahuje USB token iKey 4000, licenci obslužného software, instalační CD a poukázku na vydání osobního komerčního certifikátu.

Bezpečný klíč k datové schránce PODPISOVÝ

- je určen pro zákazníkům, kteří již vlastní komerční certifikát a chtějí v rámci akčního balíčku získat kvalifikovaný certifikát a USB token pro bezpečné uložení soukromých klíčů a certifikátů. Balíček obsahuje USB token iKey 4000, licenci obslužného software, instalační CD a poukázku na vydání osobního kvalifikovaného certifikátu.[7]

eIdentity, a.s.

Společnost eIdentity a.s.[8] nabízí na svých stránkách nejméně informací. Vznikla počátkem roku 2004 s jasnou orientací na komplexní služby v oblasti správy elektronické identity. V současné době provozuje jedno pevné registrační místo na adrese sídla firmy. Další registrační místa jsou mobilní a mohou poskytovat své služby po domluvě dle požadavků zákazníka.

[7] http://ceskaposta.cz
[8] http://eidentity.cz

Certifikační autorita eIdentity nabízí :

- kvalifikovaný certifikát
- kvalifikovaný systémový certifikát
- kvalifikované časové razítko
- komerční certifikát
- komerční serverový certifikát

Pro vydání certifikátu si musíme vytvořit zákaznický účet zvolit si své přihlašovací jméno zákaznickému účtu a určit e-mailovou adresu na kterou nám budou zaslány přihlašovací údaje. Po přihlášení vyplníme údaje objednávky a odešleme registrační autoritě. Zpět dostaneme vyjádření na návrh smlouvy a budeme vyzváni k zálohové platbě za odebranou službu. Po odsouhlasení smlouvy a přípisu platby na účet identity nám bude umožněno generování páru klíčů a volba termínu osobní návštěvy na registračním místě pro vydání certifikátu.

Vzhledem k velmi omezenému počtu registračních autorit a nejméně informací k dané problematice bych si eIdentity,a.s. pro vydání certifikátu zvolila jako poslední možnost a rozhodovala bych se mezi I.CA a Českou poštou, s.p. Já osobně bych v případě zájmu o elektronický podpis požádala o vystavení certifikátu u certifikační autoritu České Pošty, s.p., Postsignum, která disponuje nejvyšším počtem registračních míst a to 945 registračními autoritami a 7 mobilními registračními autoritami, jejíž služby si můžete objednat a veškerý proces od vystavení po instalování certifikátu provedou přímo u vás. Česká pošta navíc nabízí kvalifikovaný certifikát za 396 Kč a komerční certifikát za 348 Kč, což nejvýhodnější cena na trhu. Jen pro informaci : CA Postsignum dosáhla v měsíci květnu celkového počtu 400 000 vydaných kvalifikovaných certifikátů (www.postsignum.cz)

Postup vystavení certifikátu od PostSignum České pošty :

Pro vydání certifikátu od CA Postsignum České pošty je zapotřebí si nejprve na internetových stránkách vyplnit smlouvu o poskytování certifikačních služeb podle toho zda se jedná o fyzickou osobu OSVČ nebo právnickou osobu. Dalším krokem je vygenerování žádosti o certifikát, které provedeme online na stránkách postsignum nebo offline pomocí programu Postsignum Tool, který si stáhneme do svého počítače. Při generování žádosti se provede i tzv záloha klíče a proto generování žádosti provádíme vždy na svém počítači na kterém provedeme i následnou instalaci vydaného certifikátu. Navazujícím krokem je návštěva registračního místa certifikační autority, na kterou se dostavíme s vyplněnými smlouvami o

poskytování certifikačních služeb, vygenerovanou žádostí uloženou na USB nebo ID pokud jsme žádost uložili přes webové rozhraní a příslušnými doklady pro ověření identity. Po ověření a podepsání smluv je nám vystaven certifikát, který nám je odeslán na námi zvolenou emailovou adresu nebo uložen zpět na USB. Posledním krokem je instalace vydaného certifikátu opět přes webové stránky postsignum, kdy dochází ke spárování námi vytvořeného soukromého klíče (žádosti) s vydaným certifikátem. Po instalaci, můžeme certifikát ihned používat.

4 UPLATNĚNÍ ELEKTRONICKÉHO PODPISU V PRAXI

V poslední době stále více právních předpisů umožňuje jeho používání v oblasti orgánů veřejné správy, a to jak při komunikaci mezi úřady navzájem, tak i při komunikaci občanů s jednotlivými úřady. V současné době občané využívají elektronický podpis vůči orgánům veřejné správy především v oblasti správy daní a v obecných správních řízeních. Nutnou podmínkou pro komunikaci občanů se státní správou s použitím elektronického podpisu jsou tzv. kvalifikované certifikáty občanů.

Jako další jsou různé ekonomické softwarové programy, které nabízejí interaktivní elektronické formuláře podporující elektronické podepisování nebo přímo přenos přes datovou schránku jako například od firmy Software602, která nabízí ucelená formulářová řešení pro nahrazení oběhu papíru nejen v organizacích.

Dalším příkladem možnosti uplatnění elektronického podpisu jsou například elektronické kanály ČSOB, a.s., které nabízejí svým klientům certifikáty od I.CA a na jejich pobočkách lze tyto certifikáty i obnovovat. Elektronický podpis je totiž jednou z možností, jak autorizovat aktivní operace. K internetovému bankovnictví nabízí ČSOB produkt TWINS, který jsme již zmiňovali a obsahuje komerční certifikát pro přihlašování a kvalifikovaný pro podepisování operací.

4.1 Elektronická fakturace (e-fakturace)

Elektronická fakturace je moderní, jednoduchý, ekologický a efektivní způsob předávání daňových dokladů. Elektronickou fakturaci a vystavování daňových dokladů je možné pouze se souhlasem příjemce takového dokladu v elektronické podobě. U velkých společností je e-fakturace hojně využívána (např. již zmíněné produkty firmy Software602). Z fakturačních údajů je generován například „pdf“ dokument, který je označen pomocí elektronické značky a automatizovaně odeslán na elektronickou adresu. Podniky tak mohou ušetřit značnou část finančních prostředků.
Podle § 33 odst.2 zákona č563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, může mít účetní záznam (tedy i faktura) listinnou, technickou nebo smíšenou formu. Za technickou formu se považuje elektronický, optický nebo jiným způsobem provedený záznam, s výjimkou účetního záznamu zpracovaného v listinné podobě, který umožňuje jeho převedení do formy v níž je jeho obsah čitelný. Podle ustanovení § 33a odst. 3 zákona

563/1991 Sb. účetní záznam určený k přenosu musí být opatřen podpisovým záznamem, kterým je zaručována „průkaznost a jednoznačnost původu účetního záznamu“ ve smyslu citovaného zákona. Podpisovým záznamem se podle § 33a odst.4 citovaného zákona rozumí účetní záznam, jehož obsahem je vlastnoruční podpis nebo zaručený elektronický podpis založený na kvalifikovaném certifikátu podle zvláštního právního předpisu, anebo obdobný průkazný účetní záznam v technické formě, který zaručuje průkaznou a jednoznačnou původnost.

Obecné přínosy elektronické fakturace :

- úspora nákladů (papír, tisk, poštovné, archivace…),
- úspora lidské práce (přepisování údajů, ruční vyhledávání, zakládání, třídění...),
- zkrácení doby splatnosti (okamžitá identifikace chyb a jejich náprava),
- zrychlení procesů (zkrácení doby doručení a dalšího zpracování faktury),
- zpřehlednění procesů (snadné dohledání dokladů),
- nepotřebnost archivačních prostor (elektronická archivace),
- automatické načtení dokladů do informačního systému (zamezení vzniku chyb),
- eliminace ztrát dokumentů,
- možnost napojení na elektronický platební styk (zjednodušení procesu vystavování platebních příkazů),
- zvýšení bezpečnosti a právní jistoty (přenos i archivace dokladů v souladu s platnou legislativou),
- integrita a autenticitita (po celou dobu existence dokladu je zajištěna nezměnitelnost obsahu a věrohodnost původu je zaručena elektronickým podpisem a šifrováním),
- automatizace (celý proces od vystavení po doručení faktury je automatizován),
- kompatibilita s různými formáty (doručení dokladu v rámci libovolných informačních systémů).

Elektronický podpis u daňového dokladu jednoznačně potvrzuje vystavitele daňového dokladu, znemožňuje jakoukoliv neautorizovanou úpravu faktury po jejím vystavení a EP je podepsán pouze pdf dokument obsahující fakturu, nikoli celý e-mail s fakturou. Fakturu s elektronickým podpisem je tak možné archivovat odděleně bez doprovodného e-mailu. Pro otevření dokumentu je zapotřebí mít nainstalován program Adobe Acrobat Reader, který je k dispozici zdarma na internetových stránkách (např. www.adobe.com)

4.1.1 Ověření EP přes Adobe Acrobat Reader

Po zobrazení dokumentu se v levého části okna objeví záložka „Podpisy“, kde si můžete ověřit podepsání dokumentu a zobrazit podrobnosti certifikátu, kterým je dokument podepsán (příloha č.). Platnost certifikátu si můžete ověřit také na stránce akreditovaného vydavatele. Např. u PostSignum QCA České pošty použijete vyhledávací pole „Vyhledání podle sériového čísla certifikátu“. Sériové číslo naleznete v informacích o certifikátu v záložce „Podrobnosti“

4.2 Využití elektronického podpisu ve státní správě

Modernizovat způsob komunikace jednak uvnitř státní správy a hlavně vůči široké veřejnosti. Zavést ve větší míře elektronickou formu komunikace s občany, orgány veřejné správy a dalšími organizacemi, která uspoří čas a náklady jak na straně veřejnosti tak na straně státní správy. Se státní správou je možné komunikovat pomocí e-podatelen.

Česká správa sociálního zabezpečení

ČSSZ patřila mezi první organizace státní správy, která zavedla elektronická podání (e–Podání) dokumentů přes Portál veřejné správy (PVS). V současné době zpracovává ČSSZ 5-8 tisíc e-Podání denně, z nichž některá obsahují až stovky formulářů a jejich množství každým rokem narůstá.

Tab. č.5 formuláře, které ČSSZ přijímá elektronicky

Oblast důchodového pojištění	Evidenční listy důchodového pojištění ELDP
Oblast nemocenského pojištění	Oznámení o nástupu do zaměstnání ONZ Příloha k žádosti o dávku nemocenského pojištění NEMPRI
Ošetřující lékaři / zdravotnická zařízení	Hlášení pracovní neschopnosti HPN
Oblast pojistného na sociální zabezpečení	Přehled o výši pojistného a vyplacených dávkách PVPOJ
Osoby samostatně výdělečně činné	Přehled o příjmech a výdajích OSVČ

Elektronické podání (*e* - Podání) na ČSSZ lze uskutečnit prostřednictvím internetové sítě ve formátu XML podepsané kvalifikovaným certifikátem s využitím komunikačního kanálu PVS, VREP nebo ISDS. [9]

Generální ředitelství cel

Podání se uskutečňuje přes aplikaci webklient, kde se musíte nejdříve zaregistrovat a založit svůj účet. Po úspěšné registraci vám bude přiděleno uživatelské jméno a pracovní prostor, který bude chráněn heslem, které si sami vytvoříte. Aplikace slouží deklarantské veřejnosti jako nástroj pro zpracování elektronických celních prohlášení v režimu tranzitu, vývozu a pro podání elektronických daňových přiznání k spotřební dani. Povinnost podávat elektronické celní prohlášení v režimu tranzitu (E-TCP)je stanovena od 1.7.2006 a v režimu vývozu (E-VCP) od 1.7.2009.

Prostřednictvím aplikace webklient lze v podávat elektronicky tato daňová přiznání :

- Daňové přiznání ke spotřební dani
- Daňové uplatněn nároku na vrácení spotřební daně
- Přiznání k dani z pevných paliv

Ministerstvo vnitra

E-podatelna Ministerstva vnitra je schopna přijímat veškerá podání v elektronické podobě, která odesílatel opatří elektronickým podpisem založeném na kvalifikovaném certifikátu. Obdrží-li elektronická podatelna elektronické podání, vyrozumí odesilatele obratem e-mailovou zprávou, odeslanou na adresu, uvedenou v podání. Obsah zprávy je dán výsledkem prvotních kontrol e-podání z hlediska jeho čitelnosti, přítomnosti e-podpisu, přítomnosti viru atd. Neprojde-li e-podání některou kontrolou, e-podatelna jej nepřijme a ve zprávě je pak uveden konkrétní důvod o nepřijetí. Vypsány jsou i identifikační údaje e-podání. Vlastní potvrzení je textový soubor, tvořící přílohu elektronicky podepsaného e-mailu. Elektronický podpis se jeví jako další příloha.[10]

Ministerstvo financí – daňová správa

[9] http://www.cssz.cz
[10] http://www.mvcr.cz

Ministerstvo financí umožňuje poplatníkům pomocí aplikace EPO zasílat daňové správě elektronická podání na základě zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů a všech příslušných daňových zákonů. Podání opatřená zaručeným elektronickým podpisem odpovídají postupům definovaným v zákoně č 227/2000 Sb.,o elektronickém podpisu, ve znění pozdějších předpisů. Elektronický podpis pro účely daňové zprávy musí obsahovat podle § 11 z.č.227/2000 Sb. takové údaje, aby osoba byla jednoznačně identifikovatelná. Pro tuto jednoznačnou identifikaci osoby je používán tzv. identifikátor MPSV. Snahou projektu je zajistit podporu poplatníkům při podávání daňových přiznání, hlášení a ostatních písemností elektronickou formou.
Od 1.1.2010 je povinnost podávat souhrnné hlášení k DPH pouze elektronicky. Formulář vyplníme a odešleme pomocí aplikace EPO podepsaný zaručeným elektronickým podpisem nebo přes datovou schránku, v tomto případě elektronický podpis nepotřebujeme.

Podání lze odeslat i bez použití elektronického podpisu nebo datové schránky. Hlášení sice vyplníme a pošleme pomocí aplikace EPO, ale formulář je musíme vytisknou a do pěti dnů doručit příslušnému finančnímu úřadu.

K dalším aplikacím České daňové správy patří „Daňový portál“. Aplikace je přístupná prostřednictvím internetových stránek české daňové správy [11] a získáme na ni přístup k informacím o stavu našeho osobního daňového účtu. Informace o tom, zda finanční úřad k určitému datu eviduje na našem daňovém účtu nedoplatek, přeplatek nebo je účet vyrovnán. Vzhledem k tomu, že „Daňový portál“ pracuje s reálnými daty, vedenými u příslušných finančních úřadů, je nutné dbát na dodržení bezpečnosti přístupu k těmto údajům a pořídit si kvalifikovaný certifikát, který je nutnou podmínkou pro komunikaci se státní správou.

4.3 Informační systém datových schránek (ISDS)[12]

ISDS je informačním systémem veřejné správy ve smyslu zákona 365/2000 Sb., o informačních systémech veřejní správy. Je určen k povinnému doručování dokumentů mezi orgány veřejné moci (dále jen OVM) navzájem, mezi OVM a právnickými osobami. Pro fyzické osoby podnikající a fyzické osoby je tento způsob komunikace volitelný. Datová schránka funguje jako elektronické úložiště, které je určeno k doručování a k provádění úkonů vůči OVM a nahrazuje tak klasickou listinnou komunikaci a doručování. Datové schránky

[11] http://cds.mfcr.cz
[12] http://datoveschranky.info

zřizuje a spravuje Ministerstvo vnitra a byly spuštěny 1.7.2009. Provozovatelem je držitel poštovní licence, tedy Česká pošta, s.p. Od 1.1.2010 umožňuje komunikaci mezi právnickými osobami, podnikajícími fyzickými osobami a fyzickými osobami navzájem a od tohoto data je možné posílat přes datové schránky faktury nebo obdobné doklady o zaplacení. Od 1.7.2010 již může datovými schránkami posílat dokumenty libovolného obsahu.

Komunikace prostřednictvím datové schránky se řídí zákonem č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů a § 21 zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů (ZSDP).

Komunikace přes datové schránky je :

- rychlá – datová zpráva je doručena prakticky okamžitě,
- spolehlivá – datová zpráva se nemůže ztratit,
- auditovatelná – lze dokázat, kdo datovou zprávu poslal a komu byla doručena.

Zřízení datové schránky

- ze zákona - OVM a právnickým osobám jsou DS zřizovány automaticky,
- na žádost - Fyzická osoba si může o zřízení DS požádat a to dvěma způsoby. Pokud fyzická osoba vlastní elektronický podpis založený na kvalifikovaném certifikátu, nemusí s vytištěnou žádostí navštívit libovolné kontaktní místo tzv. CzechPOINT nebo odesílat žádost s notářsky ověřeným podpisem na ministerstvo vnitra, které přijímají žádosti o zřízení DS, ale může žádost odeslat elektronicky z pohodlí domova přímo na podatelnu ministerstva vnitra.

Přihlašování do datových schránek

základní přihlášení do DS je pomocí jména a hesla. Další možnost přihlašování pomocí certifikátu (bezpečného klíče) je pouze volitelné, nikoli povinné. Povinnost používat jméno i heslo zůstává a certifikát slouží jako další prvek autentizace.

Náklady spojené s používáním DS

Zprávy odesílané orgány veřejné moci jsou hrazeny ze státního rozpočtu. Náklady státu za provoz DS dosahují v současné době 15 Kč bez DPH za jednu datovou zprávu. Při průměrné ceně 26 Kč za doporučenou zásilku tak dosavadní úspora státu činí téměř 50 milionů korun.[13]

Zpoplatněna je tzv. „privátní“ komunikace mezi právnickými osobami, podnikajícími fyzickými osobami a fyzickými osobami, které posílají datové zprávy jiným právnickým osobám, podnikajícím fyzickým osobám a fyzickým osobám. Cena zásilky je stanovena podle zvláštního předpisu (§ 18 odst.3 300/2008 Sb.,) a hradí ji ta osoba z jejíž DS byla zpráva odeslána. Aktivace této služby se provádí elektronicky na internetových stránkách České pošty (www.ceskaposta.cz) .

Tab.č.6 Příklad úspory při používání datové schránky v komunikaci se státní správou.

Druh zásilky	Počet ks	Jednotková cena	Cena dnes celkem
Obyčejný dopis	100	10,- Kč	1 000,- Kč
Doporučený dopis	100	26,- Kč	2 600,- Kč
Doporučený dopis s dodejkou	100	32,- Kč	3 200,- Kč
Doporučený dopis do vlastních rukou s dodejkou	100	38,- Kč	3 800,- Kč
Celkem náklady dnes			10 600,- Kč

Vzhledem k tomu, že datovou schránku nám ministerstvo zřídí zdarma a komunikace směrem k orgánům veřejné moci je bezplatná je úspora nákladů při komunikaci se státní správou přes datovou schránku téměř 100%.

Zpoplatněna je tzv. „privátní“ komunikace mezi právnickými osobami, podnikajícími fyzickými osobami a fyzickými osobami, které posílají datové zprávy jiným právnickým osobám, podnikajícím fyzickým osobám a fyzickým osobám. Spuštěna byla od 1. ledna 2010 s názvem Poštovní datová zpráva. Aktivace této služby se provádí elektronicky na

[13] http://datoveschranky.info

internetových stránkách České pošty (www.ceskaposta.cz) . Použití poštovní datové zprávy je vhodné zejména v případech, kdy účastníci elektronické komunikace požadují dodání dokumentu právně prokazatelným způsobem. Poštovní datovou zprávou můžete nahradit osobní kontakt (uzavření smlouvy, ohlášení změny či některé úkony s využitím elektronického podpisu), zasílání dokumentů doporučenou zásilkou (objednávky, smlouvy, faktury, upomínky, důvěrná osobní data atd.) nebo e-mailovou komunikaci bez garantovaného dodání. Úhrada za tuto službu se provádí měsíčně, v případě, že nebyla v průběhu měsíce odeslána žádná zpráva, měsíční poplatek za využívání služby není účtován a fakturace se neprovádí.
Cena za odeslání poštovní datové zprávy (PDZ) je 13,36 Kč bez DPH a k tomu je stanoven měsíční paušální poplatek ve výši 50,- 35,- a 20,- Kč v závislosti na množství odeslaných zpráv za měsíc.

Tab.č.7 Měsíční poplatek za využívání služby PDZ:

Počet zpráv odeslaných v měsíci	Cena / měsíc (bez DPH)
1 - 10	50,- Kč
11 - 50	35,- Kč
Nad 50	20,- Kč

Daňová přiznání přes datovou schránku

Daňové přiznání je možno podat a odeslat pomocí interaktivního formuláře. Abychom ho bez problémů mohli použít je třeba stáhnout si bezplatný nástroj Software602 Form Filler, který je dostupný na internetových stránkách[14]. Software602 mimo jiné umožňuje také odeslat formulář do datové schránky, převést jej do PDF nebo vytisknout na papír. Dokumenty posílané přes DS jsou automaticky považovány za ověřené.

Interaktivní formulář daňového přiznání si můžeme stáhnout například ze serveru www.bezpapiru.cz. Na poslední straně obsahuje formulář interaktivní odkazy na další formuláře (Přehled o příjmech a výdajích pro správu sociálního zabezpečení (ČSSZ) a pro největší zdravotní pojišťovny (VZP, VoZP, OZP, MVZP...).

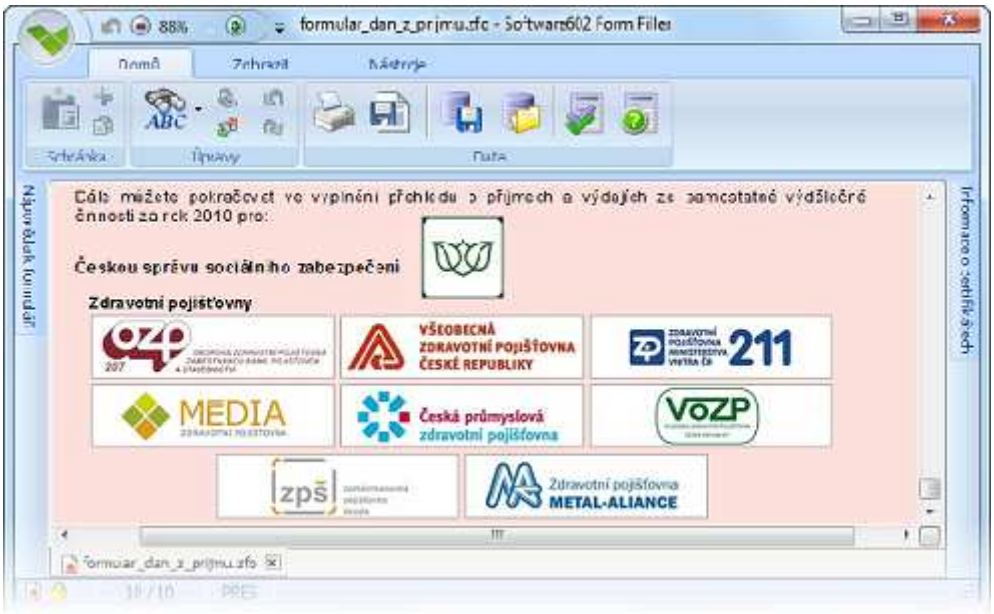
Výhody vyplňování a odesílání přiznání přes interaktivní formulář :

[14] http://www.602.cz/

- nápověda k jednotlivým kolonkám,
- automatické výpočty,
- provázání s dalšími formuláři,
- upozorní na doplnění chybějících údajů,
- snadná kontrola vyplněných dat portálem Ministerstva financí

Propojení daňového přiznání s dalšími formuláři je výhodné např. pro živnostníky. Jedním kliknutím si otevřou další formuláře, jako je Přehled o příjmech a výdajích pro ČSSZ nebo formulář pro některou z vybraných zdravotních pojišťoven. Oba přehledy získají údaje z již vyplněného daňového přiznání a lze je také jednoduše odeslat přes datovou schránku.

Obr.č. formulář Software602 (DzPFO)

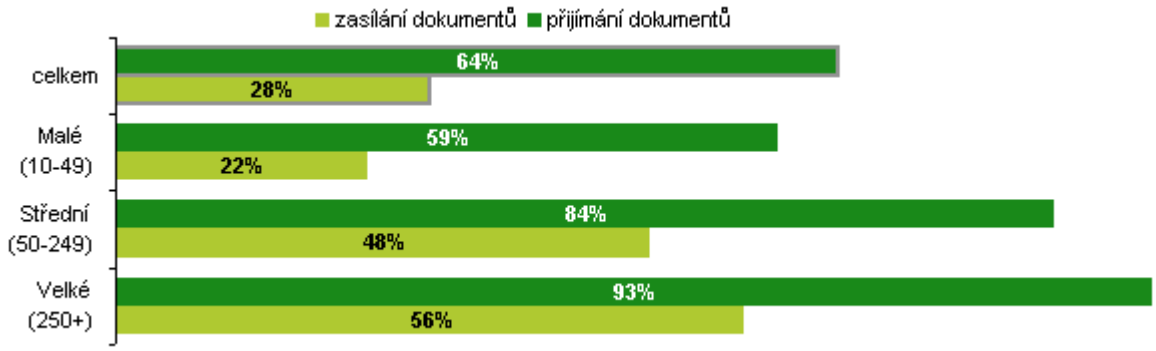


Zdroj : http://www.bezpapiru.cz/dane

Využívání datových schránek v podnicích vůči státní správě

Zajímavé jsou statistiky zveřejněné na stránkách českého statistického úřadu (ČSÚ). Z jejich šetření je v grafu č.1 patrné jak různě velké podniky využívaly datových schránek ke komunikaci se státní správou. Z výsledků šetření vyplývá, že dokumenty od organizací veřejné správy prostřednictvím datové schránky přijalo 64 % všech podniků a směrem k orgánům veřejné správy odeslalo přes datovou schránku své dokumenty 28 % podniků. Nejvíce přijímají dokumenty tímto způsobem velké podniky (250 a více zaměstnanců) a nejméně pak podniky malé (10 - 49). Je tedy zřejmé, že zasílání dokumentů přes DS není tak hojné jako jejich přijímání a v případě zasílání dokumentů jsou DS více využívány velkými podniky než malými.

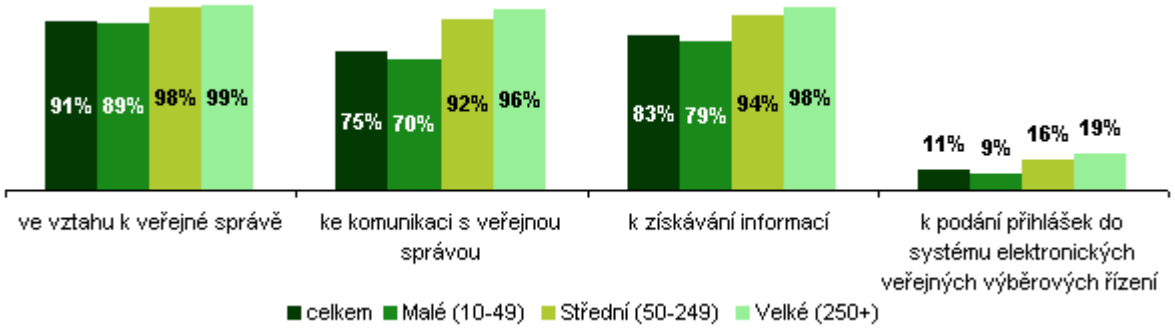
Graf 1: Podniky používající datové schránky podle účelu použití, 2009



Zdroj: Český statistický úřad, 2010

Graf č. 2 znázorňuje jak v roce 2009 využívaly podniky internet ve vztahu k veřejné správě. Jeho využívání uvedlo v lednu 2010 91 % podniků. Nejvíce používaly internet ve vztahu k veřejné správě velké podniky (99%), nejméně pak malé podniky (89 %). Obecně se dá říci, že čím je podnik menší co se týká počtu zaměstnanců, tím menší je jeho zapojení do e-governmentu. Pomocí internetu komunikovalo s veřejnou správou celkem 75 % podniků, tento relativně malý podíl je však způsoben malými podniky, jichž takto komunikuje pouze 70 %. U podniků velkých činil podle posledního šetření jejich podíl 96 %. Také elektronické podávání přihlášek je doménou spíše velkých a středních podniků . V roce 2009 podalo elektronickou přihlášku do veřejných výběrových řízení 19 % velkých podniků, 16 % středních a 9 % malých podniků.

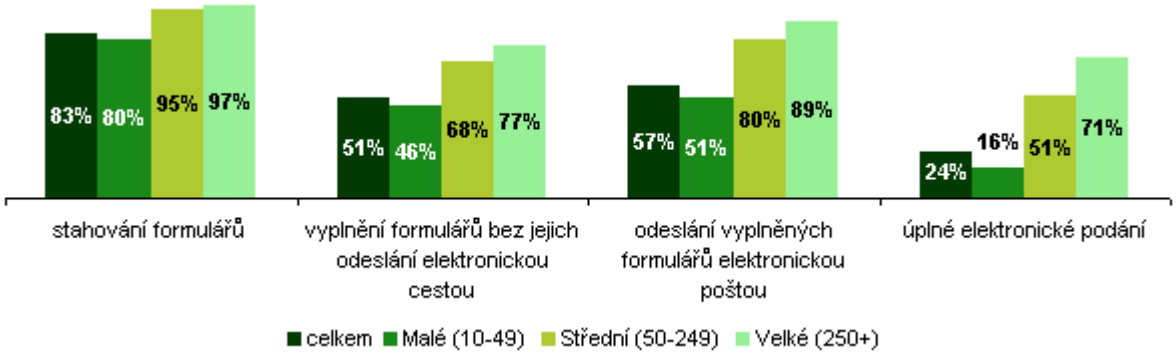
Graf 2: Podniky používající internet ve vztahu k veřejné správě, 2009



Zdroj: Český statistický úřad, 2010

Nejčastěji praktikovanou činností na internetu ve vztahu k veřejné správě podniky jak je patrné z grafu č.3 je tedy prosté využívání internetu k získávání informací z webových stránek úřadů a nejméně pak úplné elektronické podání. Stejně jako v předchozích případech, i zde platí, že čím větší podniky, tím větší je podíl těch, kteří danou službu využívají. Například v roce 2009 vyhledávalo informace na stránkách veřejné správy 98 % velkých a 79 % malých podniků a s použitím elektronického podpisu formulář podalo 71 % velkých a 16 % malých podniků.

Graf 3: Podniky používající internet ve vztahu k veřejné správě dle účelu použití, 2009



Zdroj: Český statistický úřad, 2010

4.4 Srovnání využití Elektronického podpisu a DS u vybraných profesí

Tab.č.8 : srovnání využití elektronického podpisu a datových schránek u vybraných profesí

		Soudní exekutor	Daňový poradce	Lékař
1.	Povinnost DS	ano	Ne (povinnost od 1.7.2012)	ne
2.	Využití datové schránky	80%	90%	40%
3.	Důvody stanovení využitelnosti DS	Nižší než u daň poradce Komunikuje nejen s orgány státní správy, ale i s bankami, pojišťovnami a fyzickými osobami, které DS nemají povinnou	Při jeho činnosti vidím využitelnost velmi vysokou. Veškerá komunikace spočívající v jeho práci se odehrává s orgány státní správy.	Většina komunikace probíhá s pacienty a je potřeba v písemné podobě uchovávat záznamy a zprávy. Jediné použití (většinou 1x měsíčně) může být při fakturaci a komunikaci (předání dávek) se zdravotními pojišťovnami
4.	Povinnost EP	ano	ne	ne
5.	Využití EP	80%	100%	60%
6.	Důvody stanovení využitelnosti EP	Veškerá podání uskutečněná přes DS musí být opatřena EP	Komunikuje s finančními úřady, odesílá daňová přiznání za své klienty a samozřejmě i vůči klientům využívá EP	Téměř všichni dotázaní vlastní kvalifikovaný EP, ale jeho četnost není vysoká. Používají jej komunikaci se zdravotními pojišťovnami.

Zdroj : vlastní

Vlastním šetřením, které jsem provedla pomocí dotazníku na třech profesních skupinách z řad soudních exekutorů, daňových poradců a lékařů jsem zjistila následující skutečnosti, které jsou shrnuty v tabulce viz výše.

Datové schránky pro komunikaci nejvíce využívají daňoví poradci a to z 90% veškeré komunikace a to i přes to, že zatím povinnost zřídit si datovou schránku nemají, ta jim vznikne až k 1.červenci 2012. Při své činnosti komunikují s orgány veřejné moci a jejich klientela, kterou zastupují je většinou tvořena právnickými osobami, které mají datovou schránku zřízenou ze zákona. Další skupinou, která 80% veškeré komunikace uskutečňuje přes datovou schránku jsou soudní exekutoři, kteří mají datovou schránku zřízenou ze zákona.

Komunikace přes datovou schránku není stoprocentní, a to z toho důvodu, že komunikují nejen s orgány veřejné moci, ale i s fyzickými osobami, u kterých povinnost datové schránky není. Nejnižší využitelnost datových schránek byla zjištěna u lékařů. Povinnost datové schránky nemají. Většina jejich komunikace probíhá s pacienty a to v písemné podobě a u dotázaných, kteří datovou schránku vlastní je využívána pouze ze 40% veškeré komunikace.
Soudní exekutoři mají povinnost veškerá podání přes datové schránky opatřit elektronickým podpisem a využitelnost elektronického podpisu při jejich práci je tedy vysoká a to z 80%. Téměř 100% využití elektronického podpisu uvedli daňoví poradci, kteří podávají daňová přiznání za své klienty elektronicky a proto musí být opatřena elektronickým podpisem. Elektronický podpis používají i k elektronické komunikaci se svými klienty. Většina dotázaných lékařů vlastní elektronický podpis a používají jej k elektronickým podáním přes portál zdravotních pojišťoven, ale vzhledem k tomu, že nemalá část veškeré komunikace probíhá spíše s pacienty a ta je písemná je využitelnost EP 60%.

ZÁVĚR

Cílem bakalářské práce bylo shrnout problematiku elektronického podpisu a jeho využití v praxi. Již v úvodní části je nastíněno zefektivnění řady běžných činností při použití elektronického podpisu. Na úvod navazuje druhá kapitola, kde jsem se zaměřila na legislativní rámec elektronického podpisu a vyzdvihuji nejdůležitější paragrafy zákona č.227/2000 Sb., o elektronickém podpisu a vyhlášky, které s používáním elektronického podpisu souvisí. Ve třetí kapitole jsem popsala nejdůležitější pojmy a definice. Dále se zde zabývám typy elektronických podpisů, šifrováním a jednotlivými certifikačními autoritami, které poskytují služby elektronického podpisu založeného na kvalifikovaném certifikátu, který je podmínkou pro komunikaci se státní správou. Ve čtvrté kapitole již popisuji praktické využití elektronického podpisu při komunikaci se státní správou, využití elektronického podpisu v systému datových schránek, které jsou samy o sobě určitou konkurencí elektronického podpisu.

Je zřejmé, že v dnešní době již můžeme podávat elektronickou cestou desítky žádostí. Pro ty, kdo chtějí elektronický podpis používat pouze pro základní komunikaci s úřady typu daňového přiznání nebo žádosti o stavební povolení, je mnohem jednodušší si zřídit datovou schránku, která je zřizována zdarma a podání je možné uskutečnit bez elektronického podpisu. To se ale netýká daňových poradců, kteří podávají daňová přiznání za své klienty a podaní posílají podepsaná svým elektronickým podpisem. Co se týká komerční komunikace přes datové schránky, která byla spuštěna od ledna 2010 musíme počítat s poplatky a to už tak výhodné není a je třeba zvážit, jestli pro nás nebude výhodnější si zřídit elektronický podpis. I co se týká posílání dokumentů do zahraničí, potom se bez elektronického podpisu již neobejdeme.

Můj osobní názor je, že přínos elektronického podpisu je značný, pokud se jej naučíme využívat. Na jedné straně veřejnost od zřízení elektronického podpisu odrazuje na první pohled složitá administrativa a větší počet úkonů, které vedou k získání elektronického podpisu. Na druhé straně jedna z velkých výhod, které elektronický podpis přináší je ušetření času při docházení na úřady. Díky elektronickému podpisu jsme schopni vše vyřídit jedním kliknutím v klidu domova nebo ze své kanceláře nejsme nijak časově omezeni. Je dostupné 24 hodin a 7 dní v týdnu. V dnešní době jsou elektronickým podpisem vybaveni spíše zaměstnanci větších podniků a orgánů státní moci než jednotliví občané či drobní podnikatelé. Může za to malá osvěta a vysvětlení co vlastně elektronický podpis znamená a jak funguje.

Ve své praxi jsem se s elektronickým podpisem setkala při své práci, kdy jsem pracovala jako operátor certifikačních služeb na Kontaktním místě České pošty, s.p., které vydává kvalifikované a komerční certifikáty PostSignum. Pomocí certifikátu jsem se přihlašovala do příslušných aplikací. Ze své praxe mohu říct, že většina žadatelů o certifikát přišla s minimálními informace o elektronickém podpisu a zřídit si jej přišli, protože k tomu byli donuceni buď ze strany zaměstnavatele, nebo je k tomu donutila situace, kdy určité druhy podání jako například přihlašování do elektronických systémů výběrových řízení musí být podány elektronicky a podepsány zaručeným elektronickým podpisem. Značná část žadatelů nebyla spokojena s obsáhlou administrativou spojenou s vydáním EP a měla problémy s vygenerováním žádostí o certifikát a jejich následnou instalací. Myslím si, že přínosem pro elektronický podpis by určitě bylo zjednodušení procesu, které musí žadatel podniknout, než je schopen elektronický podpis použít. I přes to si myslím, že elektronický podpis a samozřejmě i datové schránky mají budoucnost. Což dokazují např. průzkumy zveřejněné na stránkách statického úřadu. V roce 2009 přijalo dokumenty od orgánů veřejné správy 64% všech podniků a směrem k orgánům veřejné moci správy odeslalo přes datovou schránku své dokumenty 28% podniků. Od 1.1.2010 už můžou přes datové schránky komunikovat právnické osoby i fyzické podnikající osoby navzájem a posílat přes datové schránky faktury či obdobné doklady o zaplacení. Od 1.7.2010 již můžeme přes datové schránky posílat dokumenty libovolného obsahu.

SEZNAM POUŽITÉ LITERATURY

1. BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi.* 1. vyd. Olomouc: ANAG, 2008. ISBN 978-80-7263-465-1.

2. VIDINSKÝ, V.; ŠVARCOVÁ, I.; BUDIŠ, P.; LOEBL, Z.; PROCHÁZKOVÁ, B. *eGovernment bezpečně.* 1. vyd. Praha: Grada publishing, 2008. 160 s. ISBN 978-80-247-2462-1.

3. VONDRUŠKA, P.; BOSÁKOVÁ, D.; KUČEROVÁ, A.; PECA, J. *Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* 1. vyd. Olomouc: ANAG, 2002. 144 s. ISBN 80-7263-125-X.

Elektronické zdroje

Právní předpisy ČR

Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů.

Zákon č. 337/1992 Sb., o správě daní a poplatků.

Zákon č. 563/1991 Sb., o účetnictví.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Internetové zdroje

Česká pošta, s.p. Dostupné z: http://www.ceskaposta.cz

Český statistický úřad. Dostupné z. http://www.czso.cz

Datové schránky. Dostupné z: http://www.datoveschranky.info

Ministerstvo vnitra ČR Dostupné z: http://www.mvcr.cz

I.CA, a.s. Dostupné z http:// ica.cz

eIdentity, a.s. Dostupné z http://eidentity.cz

Certifikační autorita PostSignum. Dostupné z http://postsignum.cz

ČSSZ. Dostupné z http://cssz.cz

Portál ZP. Dostupné z http://www.portalzp.cz

Software602. Dostupné z http://www.602.cz

Portál veřejné správy. Dostupné z: http://www.portal.gov.cz

http://www.lupa.cz

http://wikipedia.cz

SEZNAM ZKRATEK

apod.	a podobně
atd.	a tak dále
např.	například
tzn.	to znamená
odst.	odstavec
Sb.	sbírka
DPH.	Daň z přidané hodnoty
EU.	Evropská unie
č.	číslo
obr.	obrázek
tab.	tabulka
ZoEP.	zákon o elektronickém podpisu
EP.	Elektronický podpis
DS.	Datové schránky
ISDS.	Informační systém datových schránek
DZ.	Datová zpráva
EPO.	Elektronické podání

Prohlašuji, že

jsem byl(a) seznámen(a) s tím, že na mou diplomovou (bakalářskou) práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
souhlasím s tím, že diplomová (bakalářská) práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;
bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
bylo sjednáno, že užít své dílo, diplomovou (bakalářskou) práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……

……

Jméno a příjmení studenta

Adresa trvalého pobytu studenta:

…….